SAP Solution in Detail
SAP GRC Access Control

COMPREHENSIVE, CROSS-ENTERPRISE ANALYSIS, REMEDIATION, AND PREVENTION OF ACCESS RISK

THE BEST-RUN BUSINESSES RUN SAP™

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

CONTENTS

EXECUTIVE SUMMARY

Legislators in virtually every nation have promulgated laws that mandate higher levels of corporate governance, risk management, and compliance (GRC). From the Sarbanes-Oxley Act (SOX) in the United States, to Bill 198 in Canada, to Japan's Financial Instruments and Exchange Law (the so-called J-SOX), the current regulatory environment worldwide is one that demands that enterprises take every step to ensure the integrity of their finances, their data, their processes, and their employees. Central to this is the need to control access to corporate information, functions, and processes and to ensure that there is comprehensive segregation of duties (SoD) across the entire enterprise and at all levels of corporate functioning.

Unfortunately, the cost in money and resources to ensure compliance with access control, segregation of duties, and compliant user provisioning on an ongoing basis can be overwhelming for many companies. In fact, for companies using a multitude of software solutions and applications, this task may seem virtually impossible. Establishing and maintaining a comprehensive and consistent library of SoD policies and rules, provisioning new and transferred employees, and adding new rules in accordance with changes in functions, duties, and responsibilities is a difficult challenge for any enterprise. Even companies that have deployed access control or risk management solutions can find that it is extremely difficult to translate the business definition of a particular risk into a technical definition of that risk that the solution will understand. To address these key business challenges and ensure compliance consistently year after year in a sustainable fashion, forward-looking companies are seeking enterprise-ready GRC solutions.

From the perspective of an executive and business process owner, an enterprise-ready solution must empower employees to do the right things, while enforcing that things are done right. The solution must enforce accountability and enable transparency so that business owners and executives can ultimately sign off on their attestations with confidence. As a result, compliance issues such as access control, proper segregation of duties, and compliant provisioning must be managed by a solution that spans all core business processes across all enterprise application software.
A central policy repository can then ensure consistency across the enterprise.

From an IT perspective, this enterprise readiness translates into a number of requirements. First, IT managers want an application delivered with a predefined best-practice library of comprehensive cross-process and cross-application policies. On one hand, this vast number of policy rules must be easy to enhance and to adjust as the business changes. On the other hand, rules must be granular enough to address all of the details of enterprise application software, catching all the violations without producing false positives.

Second, the solution must empower employees across the enterprise. Efficient and effective collaboration between business and IT is one of the keys to success here. Automation and dynamic workflow options not only ensure reliability and repeatability of the solution by avoiding manual errors and establishing institutional knowledge; they also accelerate processes and increase efficiency.

Third, the solution must be able to demonstrate compliance across the enterprise. It must maintain auditable records that internal and external auditors as well as regulators can use to verify compliance. Some relevant audit questions in the access control area include the following:

- What access risks are monitored?
- Which access risks have been properly mitigated?
- Who has access to a given system?
- Who granted access and when?
- Was it properly approved?

Fourth, to satisfy the needs of the IT department, the solution must have a scalable, robust, and open software architecture and be a solution that fits into any given IT system landscape. The solution should provide a range of extensibility options to meet unique business process or IT requirements. And finally, the solution must meet enterprise performance and scalability requirements.

For companies struggling to effectively meet their GRC requirements, the SAP® GRC Access Control application provides a comprehensive, cross-enterprise GRC solution that virtually shuts the door on access and authorization risks and SoD violations. Delivered with the largest and most comprehensive library of SoD rules that covers all of your business processes, SAP GRC Access Control eliminates existing risks and ensures the ongoing compliance integrity of your entire IT landscape through preventive controls and compliant user provisioning. With SAP GRC Access Control, you receive a rule set that has been developed and proven over ten years of successful implementations and backed by the deep process and industry expertise that only SAP can provide.

From supply chain to core finance operations to production-floor operations, SAP GRC Access Control delivers access risk management across your entire enterprise. It can be integrated with enterprise applications such as Oracle, PeopleSoft, Hyperion, and JD Edwards EnterpriseOne. It can even be extended to provide extensive support for legacy or custom applications. SAP GRC Access Control is available and supported worldwide in six languages.

The unparalleled rules library built into SAP GRC Access Control covers virtually all business functions and processes within the enterprise. Most companies can start with the application with only a few changes and additions to the library to cover their particular business. Making changes to the rules library is a logical and intuitive process in which all business processes and relationships can be easily expressed in the library, bridging the gap between the business definition and the technical definitions.

The cross-enterprise design and the holistic approach taken by SAP GRC Access Control provide an unprecedented level of simplicity while delivering depth and breadth of services. Only a comprehensive solution that covers the breadth (number of functional areas) and depth (number of applications) with a global solution can cover everyone in the organization and therefore simplify the way to compliance.

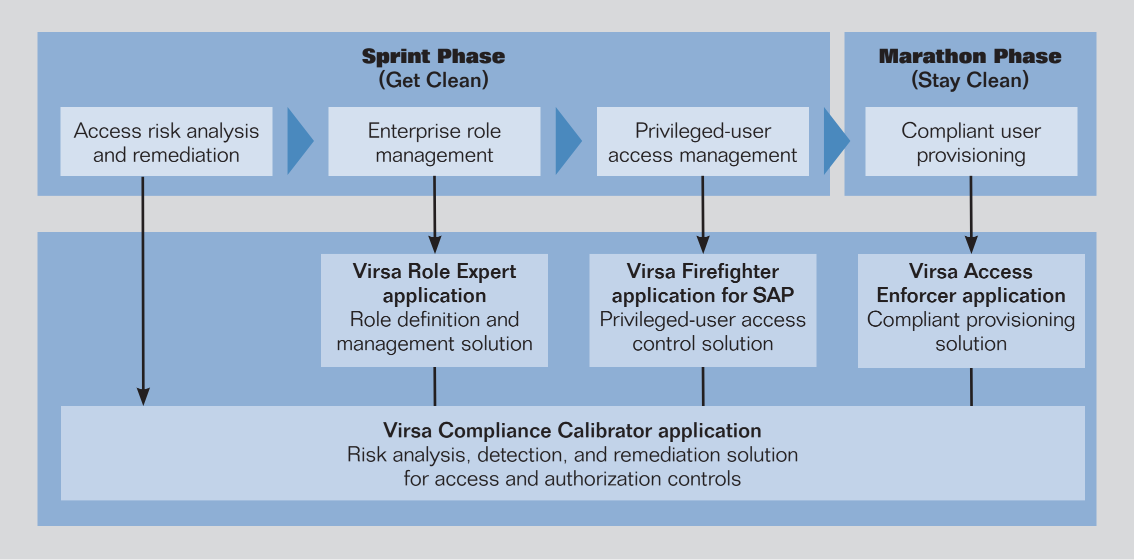
A BETTER APPROACH TO MANAGING ACCESS AND AUTHORIZATION CONTROLS

Companies spent at least US$27 billion on addressing tactical compliance issues in 2006 alone. Yet even with this investment they will remain vulnerable to risks and burdened with high costs. SAP and its partners are stepping up to the challenge by helping companies take control of governance, risk, and compliance issues and ultimately leveraging this capability as a competitive advantage. SAP will achieve this vision by delivering an integrated GRC foundation for customers to adopt in a pragmatic approach, leveraging existing IT investments in SAP software and other technologies.

In today's highly regulated environment, companies are increasingly pressured by GRC concerns while at the same time needing to drive business performance, predictability, and stakeholder confidence. The current approach to managing GRC is marked by two sets of problems: 1) highly fragmented business processes and systems that compound the cost of managing risk and compliance, and 2) little or no investment in identifying and mapping out a phased approach to comprehensive GRC management. Underlying these issues is the inherent risk in strategically coordinating and managing a wide range of IT infrastructure components that directly support the processes and systems in the GRC business environment. Organizations are deprived of a powerful tool for controlling and addressing risk effectively, while at the same time they are shifting investments and resources to non-revenue-generating activities.

SAP solutions for GRC offer a holistic approach for addressing a broad range of cross-industry and industry-specific regulations. They include the SAP GRC Access Control application that addresses a fundamental issue in many regulatory mandates. It simplifies compliance – and reduces the cost – with access and authorization control mandates such as segregation of duties or compliant user provisioning.

This market-leading application provides end-to-end automation for detection, remediation, mitigation, and prevention of access and authorization risk across the enterprise, resulting in lower costs, reduced risk, and better business performance.



Sprint Phase
(Get Clean)
Marathon Phase
(Stay Clean)
Access risk analysis and remediation
Enterprise role management
Privileged-user access management
Compliant user provisioning
Virsa Role Expert application
Role definition and management solution
Virsa Firefighter application for SAP
Privileged-user access control solution
Virsa Access Enforcer application
Compliant provisioning solution
Virsa Compliance Calibrator application
Risk analysis, detection, and remediation solution for access and authorization controls

Figure 1: Access Risk Prevention and Mitigation with the SAP® GRC Access Control Application

This document focuses on SAP GRC Access Control within the broader SAP solutions for GRC. SAP GRC Access Control offers the following functionality:

- **Access risk analysis and remediation** – SAP GRC Access Control supports real-time compliance around the clock to detect, remove, and prevent access and authorization risk and stops security and controls violations before they occur. Using live data to assess risk, SAP GRC Access Control enables your organization to identify conflicts immediately, drill down into root causes, and achieve resolutions.
- **Compliant user provisioning** – As companies provision and de-provision access to enterprise systems, they often overlook how these changes can impact SoD requirements. SAP GRC Access Control can automate provisioning, test for SoD issues, streamline approvals, and reduce the workload for IT staff.
- **Enterprise role management** – This functionality standardizes and centralizes role creation, eliminating manual errors and making it easier to enforce best practices. The application prevents SoD violations by performing a real-time simulation of the data in a production system and testing the entire SAP software landscape.
- **Privileged-user access management** – The application enables users to perform emergency activities outside their roles under a "privileged user," but in a controlled and auditable environment.

The Access-Risk Analysis Process

The fundamental principle of SoD is that the power to initiate, approve, and review activities is not held by the same person. For example, the same person should not be responsible both for authorizing to initiate a vendor payment and approving it. Access risk analysis is the process of identifying potential SoD violations. When you run an access risk analysis (against the current status) or a simulation (what-if analysis should additional permissions be granted to an individual), you generate reports presenting different types of information.

You may generate reports presenting risks; conflicts; or the use of critical transactions by the user, role, profile, or HR object you included in the analysis. By generating these reports you can identify the risk and either remove it or apply a control that mitigates the risk when the access cannot be revoked. In reality, there are thousands of business function combinations that can be categorized as access risks.

Collaboration Between Business and IT

Organizations are under more pressure than ever before as auditors raise the bar every year. However, business owners and executives who ultimately bear the responsibility for compliance don't speak the IT security language. They demand an easy-to-understand yet reliable solution. Meanwhile, chief information security officers try to meet that requirement within their budgets, even in a dynamic environment where resources are reassigned and applications are changed in the face of the latest business challenge.

SAP GRC Access Control facilitates the collaborative communication of business owners, auditors, and chief information security officers to achieve proper access control to software applications. A powerful yet elegant architecture ensures the reliable identification and mitigation of access risks across the enterprise while enabling organizations to be more efficient. It gives business owners visibility into their user access and authorizations across the enterprise that allows them to sign off on SOX attestations with confidence.

Cross-Enterprise Solution

To promote transparency, GRC solutions must span business processes. For many organizations, this also means that the GRC applications must work with all of the enterprise applications used to support those business processes. As illustrated in Figure 1, the answer is to implement a single, holistic solution that provides true cross-enterprise GRC management.

A cross-enterprise GRC solution delivers key functionality across two dimensions:

- **Breadth** in terms of business processes or functions covered, such as human resources, finance, customer relationship management, sales, and so on
- **Depth** in terms of integration with multiple business applications, which may include software from a major vendor, as well as legacy and custom applications, throughout the entire technology stack down to the data-exchange infrastructure

These two characteristics of cross-enterprise GRC enable you to address a multitude of GRC challenges, providing the following benefits:

- A holistic, cross-enterprise GRC solution addresses risk monitoring across all enterprise applications and business functions. Therefore, you need to deploy only a single GRC solution rather than multiple applications, each managing only a subset of GRC activities. A single, holistic solution significantly lowers the effort and cost of GRC for your company, freeing resources for innovation and top-line growth.
- Executives gain greater transparency into business operations across the enterprise, essential to increasing overall GRC effectiveness. Transparency overcomes the fragmentation that increases risks, reduces the effectiveness of controls, and may cause strategic misalignment and missed opportunities.
- You can automate processes that are currently manual, putting into place repeatable and auditable practices.
- You can enjoy cost-effective reporting – a huge time and money saver – and be confident that the data you submit to regulatory agencies is reliable and supportable.
- You can adjust to regulatory changes easily and speed compliance efforts, helping you bring new products to market faster than the competition – as just one example.

Cross-Functional

A cross-enterprise GRC solution should cover all business processes in your organization, ranging from the supply chain through core finance, logistics, and operations processes to customer relationship management. SAP solutions for GRC provide unprecedented coverage of business processes including procure to pay, order to cash, finance, hire to retire, payroll, production to delivery, information technology, and so on.

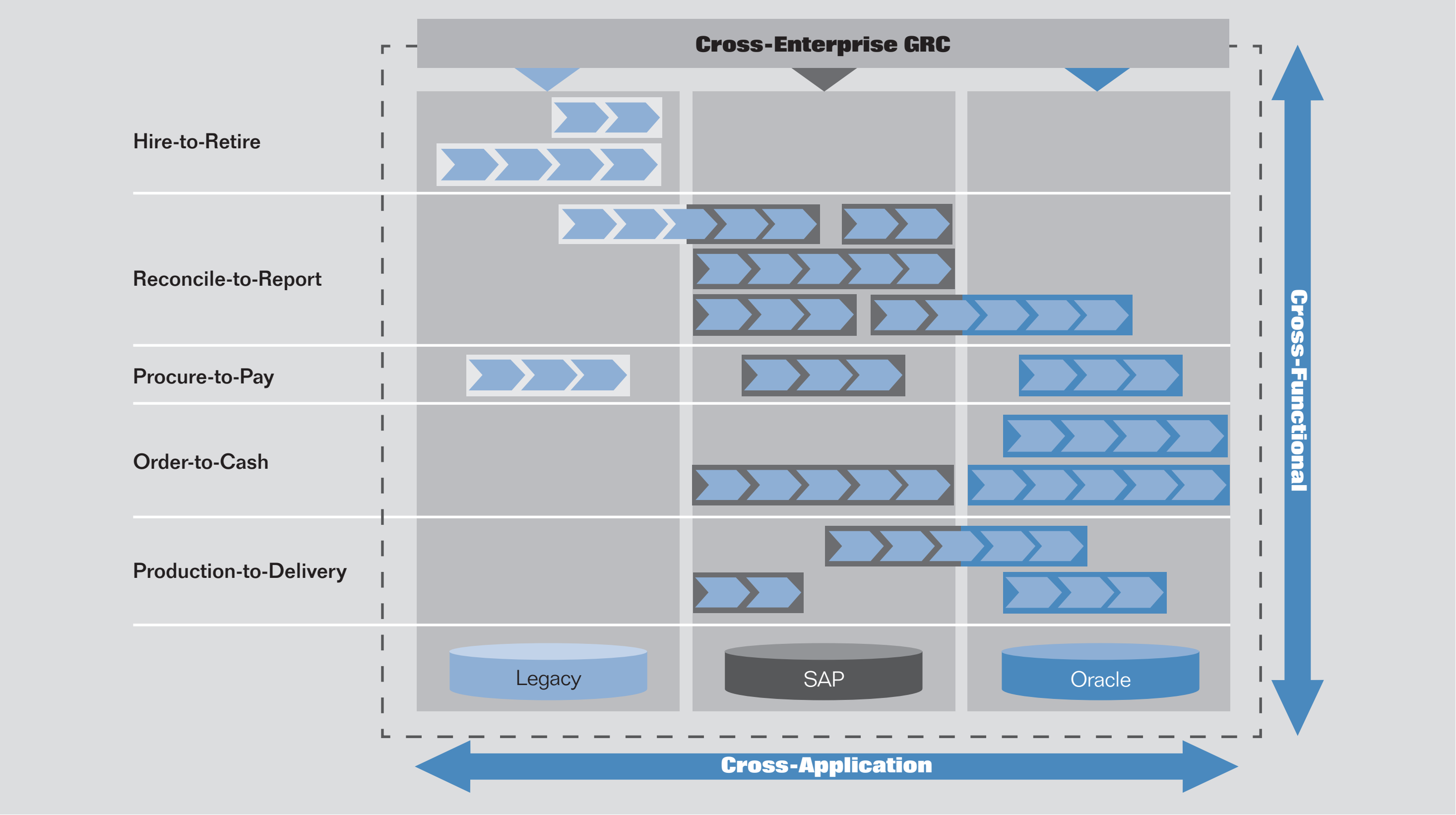


Figure 2: The Breadth and Depth of Cross-Enterprise Solutions

Cross-Application

SAP GRC Access Control delivers true multiapplication functionality, allowing you to define risks, policies, functions, and controls just once in a comprehensive GRC repository. The application then quickly maps these to the underlying business applications such as SAP, Oracle, PeopleSoft, JD Edwards EnterpriseOne, Hyperion, and so on. This approach avoids fragmentation of risk analysis, enforces all policies, and avoids duplication of effort because you do not have to recreate identical rules across application systems.

Central business rules cover end-to-end processes and uncover risks that span cross-enterprise applications.

Simplicity

The holistic approach of SAP GRC Access Control provides an unprecedented level of simplicity while delivering depth and breadth of services. Because the applications cover an unrivaled number of processes and target enterprise software, it does not matter where in the organization you are or what enterprise application software you work with. This unified approach covers SoD across the enterprise.

SAP GRC Access Control ensures compliance with a wide range of internal policies and external regulations to address the basic need of proper access management. This end-to-end solution makes access and authorization risk management and compliant user provisioning an integral part of your business and IT strategies.

Across applications and business units, SAP GRC Access Control extends the power of the largest library of SoD rules to every corner of an enterprise, to virtually every application, and to all of your critical business processes. The seamless blending of powerful software and business processes through robust workflows ensures that an enterprise will remain compliant by virtually eliminating the possibility of accidental or deliberate violations. By embedding compliance into business processes, SAP is making compliance repeatable, sustainable, and less costly for companies of all sizes in all industry segments.

Regardless of your requirements, SAP has you covered with a single solution, making SoD compliance and access risk mitigation simple for IT, and transparent for the business.

SAP GRC Access Control Overview

The following describes SAP GRC Access Control.

Access Risk Analysis and Remediation

SAP GRC Access Control supports real-time compliance around the clock and prevents security and controls violations before they occur. Implementation and deployment take about one week, after which your business can analyze real-time data, find hidden issues, and help ensure the effectiveness of access and authorization controls across the enterprise.

Analyze live data – Rather than relying upon data downloads from disparate applications, SAP GRC Access Control uses real-time data to assess risk, enabling your business to identify conflicts immediately, drill down into root causes, and achieve resolutions swiftly. Once the system is clean, you can prevent future violations by performing what-if simulations before making changes to user authorizations or roles.

Find hidden issues – SAP GRC Access Control helps organizations find potential regulatory violations that might otherwise go undetected until an audit. For example, IT can instantly analyze thousands of lines of custom code to find hidden user-access issues. This granular level of analysis enables you to find potential violations before they cause costly problems.

Remediate effectively – Real-time detection allows you to clean your system 100%. Workflow-based collaboration between business and technical users and automatic drill-down functionality allows effective resolution directly in the system. When access risk cannot be eliminated from a user's access, a mitigating control must be assigned. SAP GRC Access Control provides structured mitigation that provides real value. Only preapproved mitigating controls can be assigned – not just free text – ensuring that the required auditors' standards are met. Mitigation monitors and notification alerts can be required to ensure effectiveness of mitigating controls and provide evidence for auditors.

Manage risk across the enterprise – SAP GRC Access Control is cross-enterprise-ready. It addresses SoD issues and detects, removes, and prevents access and authorization risks across two dimensions: breadth of business processes covered and depth of integration with enterprise, legacy, and custom software applications. Only SAP GRC Access Control comes with an out-of-the-box rules library to address core processes such as procure to pay and order to cash. And thanks to the SAP partner ecosystem, a wide range of out-of-the-box connectors are available for enterprise applications from various companies, including Oracle, PeopleSoft, JD Edwards EnterpriseOne, and Hyperion. As a result, companies no longer need to deploy different compliance software for each business function and enterprise application.

Ensure segregation of duties – To increase efficiency, the application delivers the largest and most comprehensive database of SoD rules available for SAP, Oracle, PeopleSoft, and JD Edwards software. It also makes it easy for people who are not enterprise resource planning (ERP) experts to build custom rules using common business language.

The access risk and analysis functionality of SAP GRC Access Control is enabled by the Virsa Compliance Calibrator application.

Compliant User Provisioning

As companies provision and de-provision access to enterprise systems, they often overlook how these changes can impact SoD requirements. SAP GRC Access Control enables fully compliant user provisioning throughout the employee life cycle and prevents new SoD violations. Businesses can automate provisioning, test for SoD issues, streamline approvals, and reduce the workload for IT staff.

Automate provisioning workflow – SAP GRC Access Control automates even the most complex approval processes. An intuitive, self-service, Web-based interface empowers end users to request access using a context-based selection of role descriptions. The dynamic workflow engine of SAP GRC Access Control considers the functional responsibility of the requestor and the type of access request being made and automatically determines the appropriate routing for approval. The application also prevents access approval delays by routing requests to backup approvers when primary approvers are unavailable or do not respond, as well as by triggering optional detours that analyze and remove risk.

Identify SoD issues in real time – The application prevents SoD violations by performing a real-time simulation of the data in a production system and testing the entire SAP (or non-SAP) software landscape. By incorporating control activities into everyday business processes, organizations can avoid after-the-fact violation detection.

Streamline approvals – The application streamlines access requests by automatically filling each request with user identity information from an LDAP directory or HR database, thereby eliminating the need for user intervention. Approvers receive an e-mail with a direct hyperlink to the request inside the application, where they can easily view and approve the request. The SAP software then checks for security violations before automatically updating accounts.

Reduce the burden on IT – With SAP GRC Access Control, business process owners can define user access without having to learn technical terms used by the IT department. Business users can manually assign roles to requestors or model access after another user with similar roles. The application also provides self-service password reset functionality, which enables users to log on to a secure portal to reset their own passwords without assistance from IT – a feature that can reduce help-desk call volumes by up to 50%.

The compliant user provisioning functionality of SAP GRC Access Control is enabled by the Virsa Access Enforcer application.

Enterprise Role Management

SAP GRC Access Control addresses one of the roots of access control problems through a clean role design. It standardizes and centralizes role design, testing, and maintenance. As a result, the software helps eliminate manual errors and makes it easier to enforce best practices. Technical and business owners can document role definitions, perform automated risk assessments, track changes, and conduct maintenance with ease, which increases consistency and lowers IT costs.

Define auditable roles – SAP GRC Access Control puts role ownership in the hands of business users and allows for smooth collaboration with IT staff. Role owners can define which actions and permissions make up each role, trigger approval workflows, document role status, and change histories, eliminating the need for tracking spreadsheets. A role mass-import feature enables existing customers with large, manually built role sets to ramp up quickly. The application helps users redesign roles by enabling them to view all the roles in which a particular transaction is used or to compare role definitions to the way that roles are actually used in SAP applications. During the definition stage – that is, before roles are placed into production – the risk analysis and remediation functionality in SAP GRC Access Control proactively scans for, and then flags, SoD violations.

Create roles automatically – Once business owners have defined roles in the SAP GRC Access Control software, they can create them in the SAP applications with a few mouse clicks. The application leverages profile-generating functions within SAP software, eliminating the need to merge data during this process. To ensure role integrity, SAP GRC Access Control software also enables users to automatically compare role definitions to the contents of SAP applications and capture the historical reporting and analysis needed to satisfy auditors. Role owners can easily produce documentation for auditors, including role definitions, a detailed change history, and control testing results.

The role management functionality of SAP GRC Access Control is enabled by the Virsa Role Expert application.

Privileged-User Access Management

How can businesses give users privileged emergency access to enterprise systems without committing regulatory violations?

Enable fast, secure super-user logons – SAP GRC Access Control enables people to perform emergency activities outside their roles under a "privileged user" in a controlled and auditable environment. All activities are tracked and maintained from start to finish. Because the user ID is preassigned, there is no need to wait for approval before solving a critical problem.

Track super-user activities – When a user in a production system needs help, the application assigns a temporary ID that grants the user privileged yet regulated access. The application tracks, monitors, and logs every activity each super user performs under the privileged user ID. Web-based reporting provides business owners and auditors with detailed multisystem usage reports across their SAP software landscape. Activity logs track input down to the field-value level and enable easy filtering, sorting, and downloading of input information.

The privileged-user access management functionality of SAP GRC Access Control is enabled by the Virsa FireFighter application for SAP.

ENTERPRISE RULES

When addressing access risk across enterprise software, three primary goals must be met:

- The access control application must have a comprehensive rules library that covers all business functions and defines all possible risks. It must encompass the necessary level of detailed granularity to uncover all possible SoD violations, without reporting false positives.
- The rules library must be a manageable set of rules that can be maintained and adjusted easily to meet changing business requirements.
- To facilitate collaboration between business and IT, the definitions of the rules in the library must be easily accessible in commonly understood terms for business owners. They must also be capable of directly translating into all technical aspects of the various target software systems.

SAP GRC Access Control uses application-independent abstractions of risks and their underlying business functions to define the rules that identify the essential SoD violations. In its simplest form, a risk consists of two or more business functions that are in conflict.

For example, a single employee with permission to both create vendor accounts and pay vendors would constitute a business risk because that employee could create and make payments to a fictitious vendor. In this case, two business functions are in conflict: "vendor master maintenance" and "process vendor invoices." SAP GRC Access Control detects these risks in applications and across applications and prevents them on an ongoing basis.

Each business function maps to one or more application-specific actions (such as SAP software transactions, PeopleSoft components, and so on). Each action may in turn be dependent on one or more action-specific permissions (such as SAP authorization objects). These mappings allow SAP GRC Access Control to detect any access violations across various applications.

Thus, the rules architecture of SAP GRC Access Control can be viewed as a pyramid (see Figure 3). It starts at the top with a defined set of specific business risks. At the next level are all business functions that, when performed by the same person, constitute a segregation-of-duties violation. At the base, the abstract business functions are mapped to concrete technical objects in each target application.

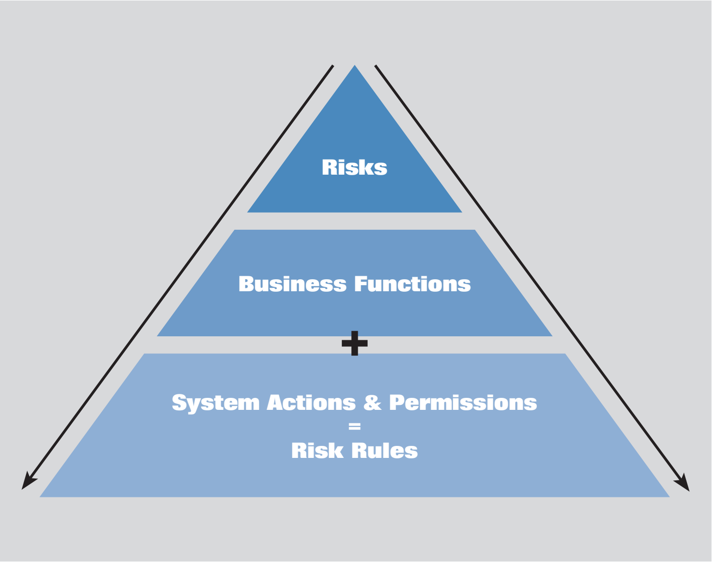


Figure 3: Business Rules – A Hierarchy of Risks, Business Functions, and System-Level Actions and Permissions

Finally, for execution, SAP GRC Access Control dynamically generates a much larger set of rules. These generated rules represent all possible permutations of all actions and permissions of every business function against all actions and permissions of every other business function for a given risk.

Benefits of the Rules Architecture

A primary benefit of the rules architecture is that risks and business functions are defined in commonly understood terms, thereby encouraging regular business users to use SAP GRC Access Control. This architecture allows collaboration between the business and IT sides, with business managers taking ownership of proper risk definition and ultimately owning the compliance responsibility.

With one central and system-independent definition of the policies (risks and business functions) across the enterprise, risks and business functions need to be defined only once. SAP GRC Access Control maps those risks and functions across multiple target applications, avoiding fragmentation and duplication of effort. A central rule set ensures consistent policy and checks for violations that may be spread over multiple applications. This is critical for businesses that are running applications from multiple vendors. For example, it would be possible to create vendors in an SAP application and pay vendors using a PeopleSoft product. Unlike other available offerings, SAP GRC Access Control can check the rules across both applications to detect that risk, which would otherwise go unnoticed.

The top level of the rules pyramid in commonly understood terms is manageable in size and ensures consistent policy across all enterprise software. Even with the expansive prepopulated rules content, it is easy to maintain the rule set using the powerful rule architect tool to make changes and add new rules. The rules architecture is designed specifically to allow updates to the rules library to be made at the abstraction level of risks and business functions. Instead of defining risks and functions at the IT systems level, business owners can define risks and functions in commonly understood terms and have those definitions transformed into precise definitions at the systems level.

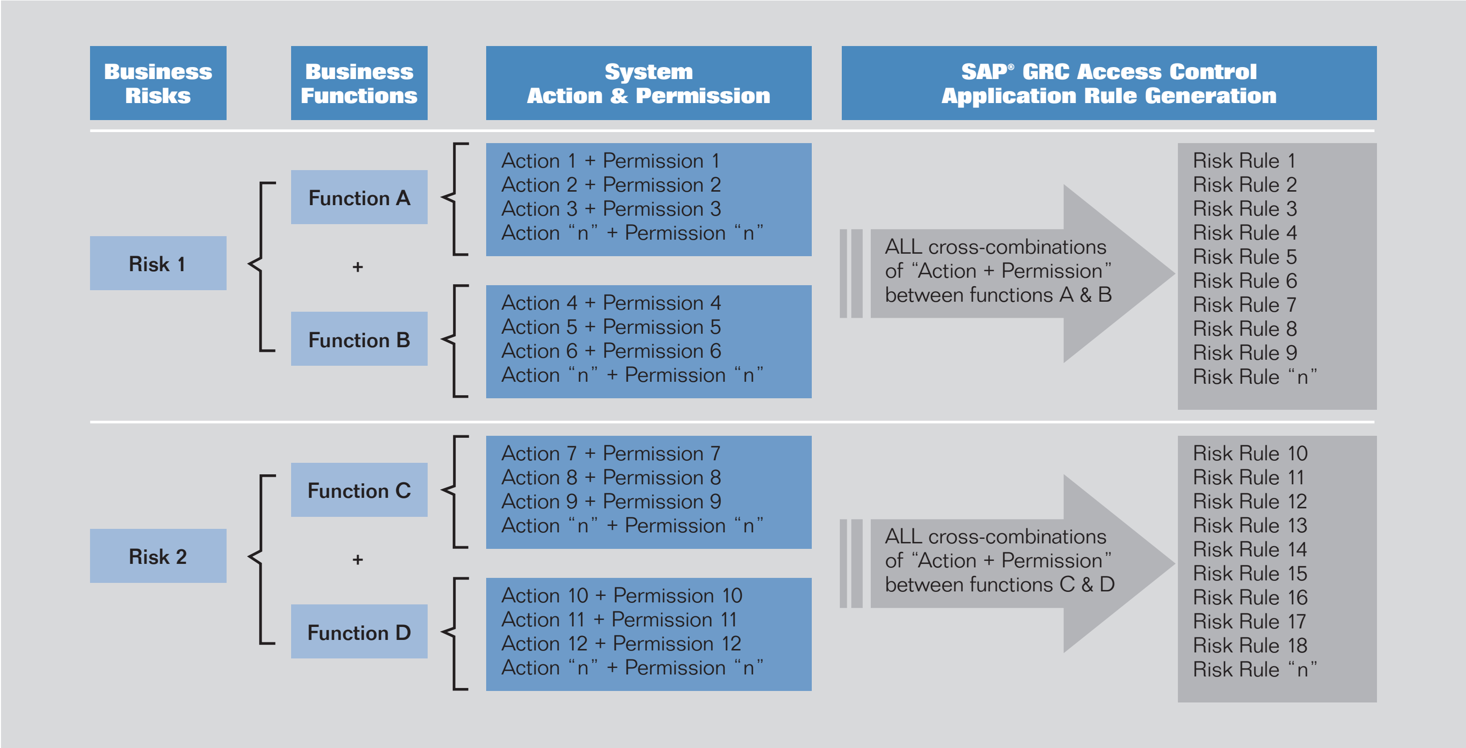


Figure 4: Automated Rule Building

Largest Library of Predefined Rules

SAP GRC Access Control comes with an unrivaled set of rules for enterprise software products. The powerful and comprehensive rules library can easily generate well over 100,000 rules out of the box for use with SAP applications. It can generate a similar number of rules for enterprise software from other major vendors. In addition, the rules set can be expanded to include extensive support for legacy and custom applications.

The table below shows the number of business risks addressed, as well as the breadth of business processes covered.

More Than SoD

The SAP GRC Access Control rules architecture lends itself to more than just identifying SoD violations. SAP GRC Access Control can easily perform the following comprehensive access risk analysis:

- **Segregation of duties** – Risks defined as two or more business functions, mapped to system-specific actions and permissions, typically make up the rule set for the segregation-of-duties solution.
- **Critical actions or critical permissions** – Definition of risks as just one business function with just one (or more) actions or even just one (or more) permissions allows customers to monitor who is accessing which critical functions. For example, a rule containing just a business function called "payroll" and mapped to the permission or authorization object within the HR application will allow compliance managers to identify reliably all users accessing the HR payroll function.
- **Protection of sensitive information** – It is possible to set up special rules to control information security and privacy, for example in human resources (employee information security) or customer relationship management (customer information security). Through so-called supplemental analysis, you can add additional rules to provide further constraints on whether or not a violation condition is raised.
- **Critical roles or profiles** – Likewise, it is possible to flag critical or insider roles or profiles and then monitor the assignment of these critical roles.

Cross-Enterprise Rules Library Delivered out of the Box

SAP® GRC ACCESS CONTROL APPLICATION				
SAP	**Oracle**	**PeopleSoft**	**JD Edwards**	**Hyperion**
■ HR ■ Procure to Pay ■ Order to Cash ■ Finance – General Accounting – Project Systems – Fixed Assets ■ Basis, Security, and System Administration ■ Materials Management ■ Advanced Planning and Optimization ■ Supplier Relationship Management ■ Customer Relationship Management ■ Consolidations	■ HR ■ Procure to Pay ■ Order to Cash ■ Finance – General Accounting – Project Systems – Fixed Assets ■ System Administration	■ HR ■ Procure to Pay ■ Order to Cash ■ Finance – General Accounting – Fixed Assets ■ System Administration	■ HR/Payroll ■ Procure to Pay ■ Order to Cash ■ Finance – General Accounting ■ Consolidations	■ Custom Rules

Rule Architect

The rule architect allows you to enhance the out-of-the-box rule set to incorporate unique conditions of the organization, make industry-specific enhancements, and meet other custom needs. The rule architect is also used to create rules for custom and legacy applications for which no out-of-the-box rule sets exist.

With the rule architect, business analysts can easily adapt the rules library to changes to the enterprise, changes to the business environment in which the enterprise operates, and changes to the regulations and laws that govern the business.

With the rule architect, you can see all the rules shipped out of the box and the risks and business functions, as well as the mappings to system actions and permissions. When adding or altering rules, you use the rule architect to identify the combinations of transactions and authorization objects that represent conflicts. The rule architect provides all the tools you need to define SoDs and business processes and generate the rules used during access risk analysis.

Organizational Rules

This feature allows you to adjust the granularity level at which access risks can be analyzed. Instead of running a global risk analysis against all organizational entities, organizational rules allow you to filter an access risk analysis based on those entities (for example, subsidiaries). The purpose of organizational rules is to eliminate false positives that might be detected otherwise with a less sophisticated standard risk analysis.

In this context, a false positive is defined as an SoD conflict identified at the transaction level for a user, role, profile, or HR object that can be eliminated when analysis is run at the authorization object level. This can be done using organizational rules, which allow you to filter a risk analysis based on organizational levels.

For example, if you run an analysis on a user, it may identify an SoD for conflicting transactions such as FB01 (posting a payment) and XK01 (create vendor). Applying an organizational rule to the analysis might remove the conflict if the user being analyzed has access to FB01 for one organizational level – for example, US01 (company code BUKRS) – and access to XK01 for a different company code. By applying an organizational rule you have eliminated the false positive.

Organizational rules are an important extension if you are managing SoD by separating responsibilities through organizational levels and not business functions. This approach is typically used in shared-service centers. You can also limit the users included in an access risk analysis by specifying an organizational rule ID. Organizational rules determine which users are included in the risk analysis by organizational entity values.

Organizational rules allow you to isolate access risk analyses to specific organizational entities. Organizational rules are used when running a user-based risk analysis and determine which users should be included in a risk analysis when the organizational rule ID is specified.

When you apply an organizational rule to a user-based risk analysis, the risk analysis report contains all SoDs for the users included in the analysis with the exception of the risks specified in the organizational rule.

SAP GRC ACCESS CONTROL SOFTWARE ARCHITECTURE

The design of the architecture for SAP GRC Access Control delivers a level of performance, integration, extensibility, and scalability unmatched in the market. Through real-time agents (RTAs), Web services, and open interfaces, SAP GRC Access Control can be extended to virtually any application, SAP and non-SAP alike. In addition, the application can easily be integrated with other solutions, such as user-provisioning applications, to provide the same high level of compliance and risk mitigation to users generated via those applications.

Architecture Overview

SAP GRC Access Control consists of the core Java module as well as one or more RTAs that allow it to communicate to the target application. Where real time isn't feasible or desired, an offline file extraction (EXT) can be used. One centralized rule set within the GRC repository allows the application to analyze access and authorization risks across the enterprise, for a wide range of enterprise software systems and essential business processes.

The SAP NetWeaver® Platform

SAP GRC Access Control is powered by the SAP NetWeaver® platform, the basis for all SAP applications. The common platform allows for a low total cost of ownership by providing many common services and for easy integration with non-SAP applications. SAP GRC Access Control is implemented in Java on the Java Web application server functionality of SAP NetWeaver.

These are some of the SAP NetWeaver components and services used by SAP GRC Access Control:

- SAP user-management engine component (UME) – Contains user and authorization information for Java applications running on the Java application server of SAP NetWeaver. User data (user accounts, authorization, and access data and permissions) for SAP GRC Access Control comes from the SAP user-management engine, and user access to SAP GRC Access Control is controlled by the user-management engine.

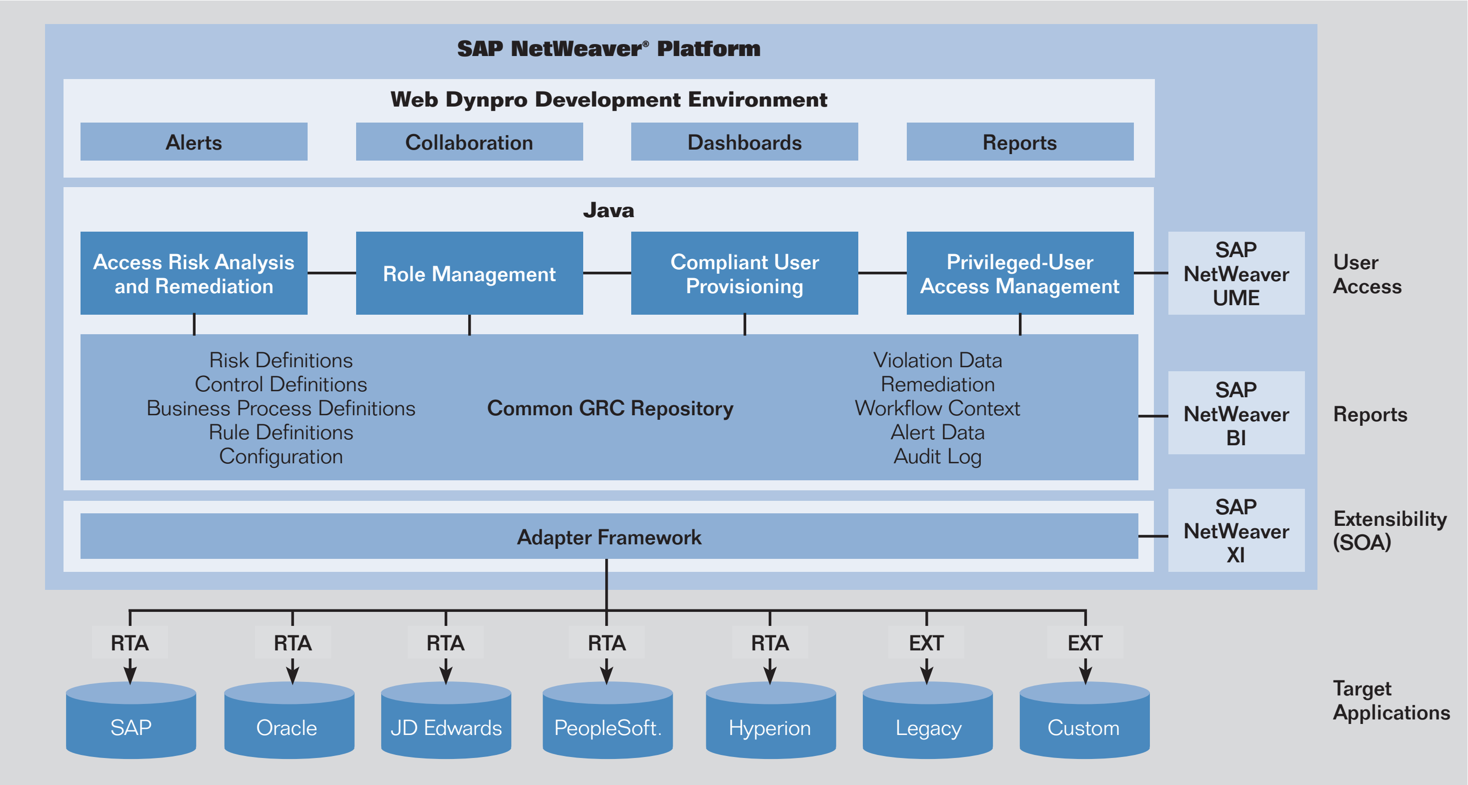


Figure 5: SAP® GRC Access Control Application Architecture

- SAP NetWeaver Business Intelligence (SAP NetWeaver BI) component – Optionally provides additional reporting functionality that goes beyond the extensive list of built-in reports (ideal for complex custom reporting and analysis)
- SAP NetWeaver Exchange Infrastructure (SAP NetWeaver XI) component – Optionally provides the Web services infrastructure for applications that could utilize the Web services exposed by SAP NetWeaver

  SAP GRC Access Control uses SAP NetWeaver XI to call Web services of other applications. For example, a customer's custom and legacy applications may expose Web services to provide user and authorization information that needs to be analyzed for SoD violations.

The Core Java Application

SAP GRC Access Control is implemented in Java on the SAP NetWeaver Application Server component. SAP GRC Access Control allows for real-time connections to the target enterprise software to be risk-analyzed. Non-real-time solutions typically require downloads of user and access information that require far more time, storage space, administration, and system resources. Moreover, unless you are downloading hourly, the system delta between downloads leaves considerable room for error or access violations. The SAP GRC Access Control application has none of these drawbacks.

RTA: The Enterprise Software Real-Time Agent

SAP GRC Access Control provides a flexible and elegant solution for real-time integration to your ERP system. SAP provides the RTAs for all mySAP™ Business Suite applications. A wide range of real-time agents is available from the SAP partner ecosystem for non-SAP enterprise application software including Oracle, PeopleSoft, JD Edwards EnterpriseOne, and Hyperion.

The Java application communicates with the target enterprise software through the RTA. RTAs can perform a variety of functions depending on which activity within SAP GRC Access Control initiates the call to the RTA, including:

- Run a risk analysis or simulation against the enterprise application software[1]
- Run controls that prevent users from bypassing SAP GRC Access Control when creating or changing user access
- Provision users into the target enterprise software
- Create IT roles in the target enterprise software

Adapter Framework and RTAs

The adapter framework is the central component of the SAP GRC Access Control application where connections to multiple enterprise software systems are defined and maintained. The adapter framework provides a common runtime environment for the risk analysis of different ERP systems. This includes connectivity to different systems or applications, service invocation, data mapping, and unification.

The RTA is a back-end counterpart that resides in the target systems. Depending on your system landscape, there are different approaches you can take in integrating to your ERP system:

- **Real time** – SAP GRC Access Control provides prebuilt RTAs specific for SAP software. For all SAP applications, the RTA is an ABAP™ programming language component embedded in the SAP application. In addition, SAP GRC partners provide prebuilt RTAs for a variety of non-SAP enterprise software, including Oracle, PeopleSoft, JD Edwards EnterpriseOne, and Hyperion. You can also create custom RTAs using stored procedures or Web services. Finally, you can create custom queries to access your legacy system database directly.

[1] The risk analysis can always be substituted by an offline file extraction (EXT) if an RTA is not desired or available for the specific target software.

- **Offline or extraction** – SAP GRC Access Control provides a file adapter that uploads flat files extracted from your legacy system. (The flat file can be in a delimited format using any delimiter such as a comma or tab). The file adapter reads the file, maps the data to the generic structure format, and loads it to the generic data structure of SAP GRC Access Control.

RTA USAGE	TYPE
Prebuilt for SAP	BAPI® programming interface
Prebuilt for Oracle	Stored procedure
Prebuilt for PeopleSoft	Web services
Prebuilt for Hyperion	Web services
Custom-built for direct access to legacy system database	Query
Custom-built for upload file extraction to legacy system	Flat file (delimited)

The adapter framework and RTA establish the link or connection to the back-end system. The Java application then executes the RTA to access user and authorization data, and maps data to the generic data structure of SAP GRC Access Control.

Access Risk Analysis, Remediation, and Mitigation

SAP GRC Access Control provides out-of-the-box real-time risk analysis for SAP applications, as well as the major enterprise systems from Oracle, PeopleSoft, JD Edwards, and Hyperion (via partner RTAs) along with prebuilt rule sets for all five.

SAP GRC Access Control also supports offline connectivity to legacy and custom systems through the adapter framework and the rules architect, which can be used to define custom connections (adapter framework) and custom rules (rules architect) for those systems.

Application-Specific Functionality

Privileged-User Access Management

Auditors are cracking down on the blanket access typically given by IT to support staff with temporary super-user needs. But how can businesses give users emergency access to enterprise systems without committing regulatory violations? The privileged-user access management function of SAP GRC Access Control enables users to perform emergency activities in SAP applications outside their roles under a controlled and auditable environment. All activities are tracked and maintained from start to finish.

When a user in a production system needs help from an IT super user, the application assigns a temporary ID that grants the user temporary, broad, yet regulated access. The user simply logs on to the application's main console, where a new session is opened under the temporary ID. Because the ID is preassigned, the user never needs to wait for approval before solving a critical problem.

Without placing a burden on the logging functions of SAP applications, the privileged-user access management function of SAP GRC Access Control tracks, monitors, and logs every activity the user performs under the temporary ID and gathers logging information from various sources, including the following:

- **Statistical records and user activities (STAT)** – Activities are logged and categorized by transaction and user in statistical records.
- **Change documents (CDHDR)** – Changes are captured in so-called change documents, that is, entries into the CDHDR table.
- **Transactions** – All transactions that are successfully entered are reported, whether any updates were made or not.
- **Programs executed** – If transactions SA38 or SE38 are executed and a program is run, the program name is reported.
- **Table updates** – If table updates are made, the transaction used to update a table (SE16, SM30) is reported. (Table name and table entries changed are reported if table logging is enabled.)

This detailed reporting enables business owners and auditors to track usage. Activity logs track input down to the field-value level and enable easy filtering, sorting, and downloading of input information. The application also automatically sends notifications of usage to security administrators and can e-mail detailed logs to responsible parties for review.

With the privileged-user access management function of SAP GRC Access Control, security administrators retain complete control over the use of IDs – including those of super users. They can allocate users, assign access rights, configure notification policies, and perform detailed auditing. Because the privileged-user access management functions of SAP GRC Access Control is already embedded in SAP applications, it is easily deployed and administrated and delivers a user experience consistent with other SAP software.

Enterprise Role Management

SAP GRC Access Control can be a centralized repository for enterprise-wide role documentation management, including SAP and non-SAP applications.

In addition, the application offers a number of advantages for role definition and management, including:

- A defined methodology for role definition
- Suggestions for adherence to naming convention and syntax, ensuring consistency
- Classification of roles into functional areas, business processes, and subprocesses for ease of administration
- Tailoring of roles through simplified definition of custom fields
- Assurance that roles are created and approved by defined rules using the approval workflow

In addition, in SAP software environments, the application provides for SoD risk analysis and automatic role generation in the SAP software target system.

The enterprise role-management function of SAP GRC Access Control provides compliant role design and helps ensure that there are no SoD violations. Roles designed in the software are populated to the profile generator after the roles have undergone risk analysis and approval.

EXTENSIBILITY

SAP GRC Access Control supports open interfaces and Web services, allowing you to fully integrate it into your IT environment. Through these interfaces and services, you can extend the benefits of SAP GRC Access Control to virtually all of your business applications and processes.

Import and Export Interfaces

SAP GRC Access Control provides a variety of interfaces to import or export preexisting content such as risks, business functions and rules, and user roles.

Rules Information

You can import business functions, business processes, and risks into the SAP GRC Access Control application from a number of sources including a Microsoft Excel spreadsheet. The following are sample definitions of the file format for the various components for the rule definitions.

Organization Information

You can import organization-level information into the SAP application via text files (for example, Microsoft Excel files) uploaded via the rule architect utility.

Role Information

You can import role information into the SAP application via files (for example, Microsoft Excel files) uploaded with the rule architect utility.

Web Services

Through its adapter framework, which can call other Web services, SAP GRC Access Control can participate in any solutions using enterprise service-oriented architecture (enterprise SOA). Business applications such as PeopleSoft and Hyperion that expose the required user and authorization information as a Web service can easily be added to the SoD risk analysis.

Sample Definition of File Format

FUNCTION DEFINITION

Function ID (8)	Language (2)	Description (132)	Scope (1)
AO01	EN	AO01 – APO Supply & Demand Planning	S
AO02	EN	AO02 – APO Maintain Model	S

Values in parentheses show field length. Scope can be “S” (Single) or “C” (Cross).

When creating import records, you should group functions into risks and link each risk to a business process. You should also provide a risk description and identify the risk level.

FUNCTIONS LINKED TO BUSINESS PROCESS

Risk ID (4)	Function 1 ID (8)	Function 2 ID (8)	Function 3 ID (8)	Function 4 ID (8)	Function 5 ID (8)	Business Process ID (4)	Priority (1)	Status (1)
A001	AO02	AO01				AP00	1	1
A002	AO03	AO01				AP00	1	1
A003	AO04	AO01				AP00	1	1
A004	AO05	AO01				AP00	0	1

RISK DESCRIPTION AND LEVEL

Risk ID (4)	Language (2)	Risk Description (132)	Detail Description (1000)	Control Objective (1000)
F001	EN	Maintain fictitious GL account & hide activity via postings	Create fictitious GL account and generate journal activity or hide activity via postings entries	
F002	EN	Alter cost center and process unauthorized cost transfers	Alter a cost center without authorization and process unauthorized cost transfers to this cost center, possibly	

In addition, SAP GRC Access Control exposes a variety of Web services that other applications can consume, extending and embedding GRC functionality to those applications. For example, if a business already has a ticketing system for handling user requests, then this ticketing system could reach the access control functionality through its Web services.

Other SAP GRC Access Control functions accessible via Web services include:

- Analyze SoD risk for user, role, profile, organization level, and HR organization
- Create, update, delete, and search for a risk
- Create, update, delete, and search for a mitigation and mitigation control assignment for a user, role, or profile
- Create, update, delete, and search for a business function
- Get transaction usage for a user
- Submit a user provisioning request (such as from a ticketing system or identity management system)
- Provide audit trail information for a submitted request (including request status)
- Get all provisioning information for a user, such as whether the user was created, changed, or deleted, or a role was added or removed

Identity Management Integration

Identity management integration is based on the Web services exposed by SAP GRC Access Control. Any existing identity provisioning management solution, whether from a third party or a proprietary system, can be extended from basic-user provisioning to compliant user provisioning. SAP GRC Access Control adds the intelligence to the user-provisioning workflow to check for any SoD violations and handles the potential mitigation steps.

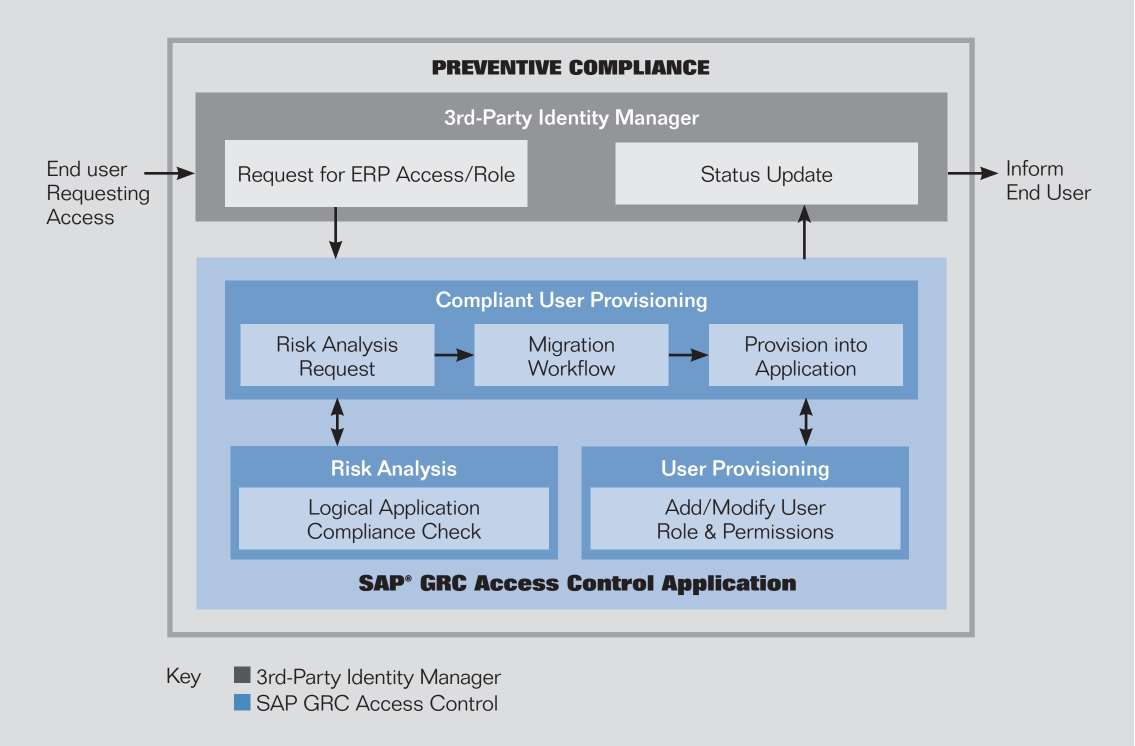

PREVENTIVE COMPLIANCE
3rd-Party Identity Manager
End user Requesting Access
Request for ERP Access/Role
Status Update
Inform End User
Compliant User Provisioning
Risk Analysis Request
Migration Workflow
Provision into Application
Risk Analysis
Logical Application Compliance Check
User Provisioning
Add/Modify User Role & Permissions
SAP® GRC Access Control Application
Key
3rd-Party Identity Manager
SAP GRC Access Control

Figure 6: Process Flow for Extending GRC to a Third-Party Identity Management Solution

WORKFLOW AND AUTOMATION

The orchestration functionality in SAP GRC Access Control focuses on system-to-system communication, supporting compliance processes that depend on integrating diverse software via Web services. Yet the ability to coordinate and automate work done in concert by software and by people – a process often referred to as workflow – can streamline more processes than just integration scenarios alone.

SAP GRC Access Control delivers a single, robust workflow engine designed to guide human activity and enforce policies through automated and structured processes – or sequences of activities – across a wide range of business tasks including:

- **User access request**
  Any user can request access for personal use or on behalf of others (for example, by a hiring manager for a new hire).
  This triggers a workflow that orchestrates the approval of the access request by a dynamically determined set of responsible individuals – typically the direct manager, role owner, and IT security. It will intersect these human activities with automated risk analysis and require approvers to mitigate any potential access risks found prior to approval.
  This user-requested workflow is not only triggered by an individual requesting access through a self-service Web page, but it can also be configured to use the mySAP ERP Human Capital Management (mySAP ERP HCM) solution as the authoritative source and trigger a workflow with each relevant HR event.
- **Role approval**
  Workflow facilitates the approval process within the role design and maintenance functionality of SAP GRC Access Control. It submits roles for approval to business managers and role owners to ensure proper sign-off before roles are added or changed in target software systems.
- **Risk mitigation**
  Assigning mitigation control through compliant user provisioning enabled by Virsa Access Enforcer also triggers an approval workflow.

You can customize workflows to reflect company requirements or policies.

The embedded workflow engine delivers dynamic and configurable workflow solutions, as follows:

- The flow of activities can be configured based on various attributes of the triggering request or activity. (For example, a user-access request can be routed based on type of access requested, position of requestor, and so on.)
- The workflow engine can have an escape route defined if the workflow participants (for example, approvers) cannot be found.
- The workflow engine can configure workflow so that certain requests can branch into multiple parallel approval paths.
- The workflow engine can have detours on predefined conditions.
- The workflow engine can configure certain participant activities at each stage (for example, those of approvers).
- The workflow engine can have dynamic approval determination at each stage.
- Workflow participants can forward or reroute a request at certain stages, if rerouting is allowed at that stage.

Administrators have a full overview of all workflows in progress and can approve them at any stage. For auditing, the workflow keeps a full audit log of all activities. For user provisioning, a provisioning log is available through the compliant user provisioning function.

SYSTEM LANDSCAPE

No two enterprise software system deployments are exactly alike, but most enterprises have a system landscape that consists of a development ERP system, a quality assurance ERP system, and a live production ERP system. All modifications, upgrades, and additions are first made to the development system. Once the changes have been stabilized on the development system, they are transported to the quality assurance system for acceptance testing with a subset or snapshot of the production data and then to the production system for actual use.

SAP GRC Access Control accommodates a wide range of system landscapes.

SAP Software–Only System Landscapes

Within a typical SAP software system landscape, how does a customer integrate SAP GRC Access Control functionality into the IT environment? Figure 7 shows the appropriate deployment of the applications across this landscape.

Basic Landscape

Virsa Compliance Calibrator is typically deployed in all systems that require risk analysis: the development (DEV), the quality assurance (QA) system (especially if a subset of production data is used for testing), and of course the production system (PROD). It provides the basis for access risk analysis, risk remediation, and mitigation, as well as prevention, and is the fundamental component for the other SAP GRC Access Control applications that rely on its risk analysis.

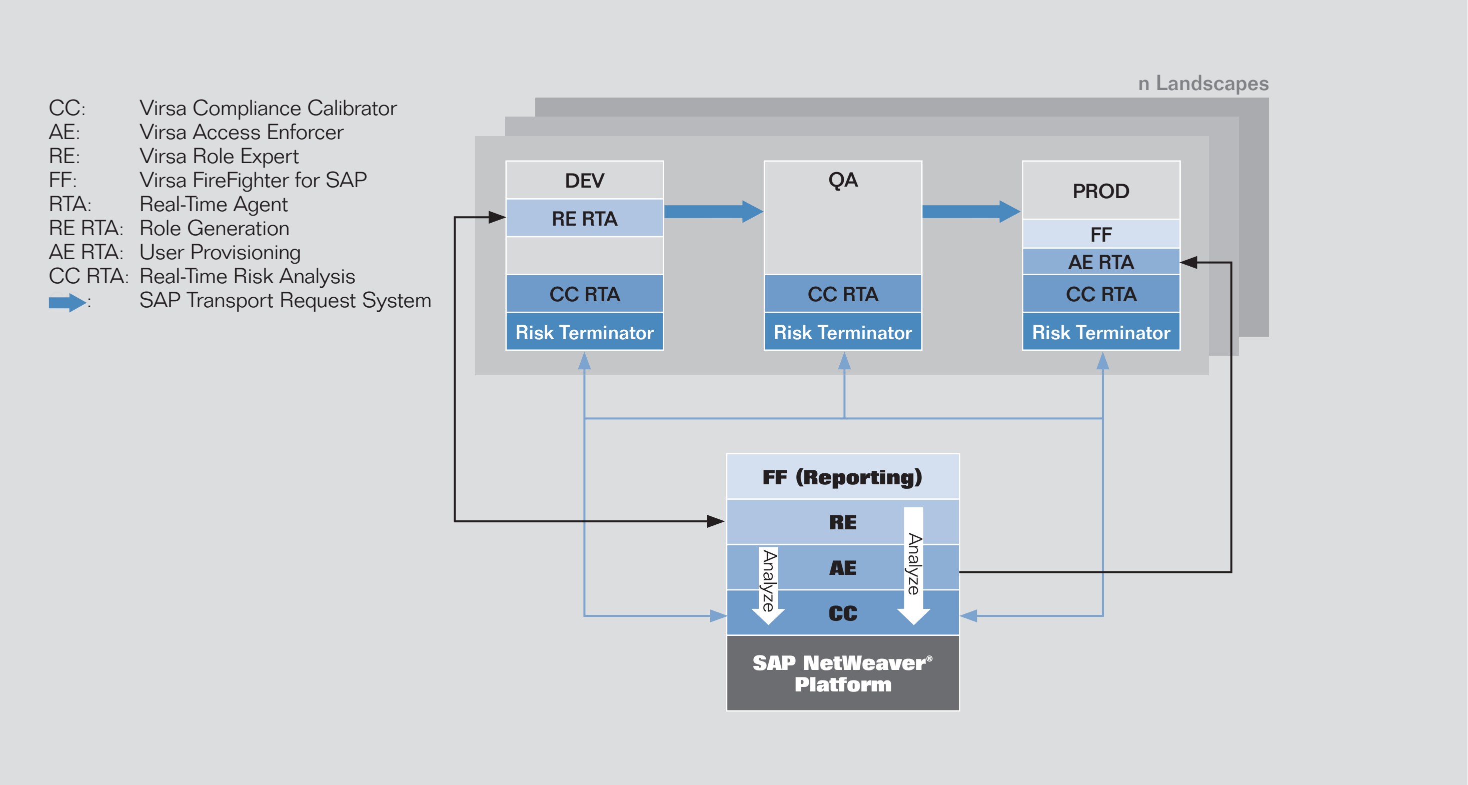


Figure 7: SAP® GRC Access Control Application System Landscape for a Typical Installation

The RTA for Virsa Compliance Calibrator also contains the **risk terminator** functionality. This is preventive functionality that ensures that system administrators, IT security staff, role managers, and other users with high authorization levels for provisioning privileges cannot bypass SAP GRC Access Control risk analysis and mitigation using standard SAP user-management functionality.

Virsa Role Expert is a design-time tool that manages all role definitions. The application is typically deployed against the development system. The Virsa Role Expert RTA for SAP software systems (RE RTA) can retrieve any existing roles from the development system into the role document-management repository. Virsa Role Expert then manages the initial role cleanup and the ongoing role definition and maintenance using a structured process. Virsa Role Expert relies on the automated access-risk analysis functionality of Virsa Compliance Calibrator. Through the RE RTA, it ensures automatic role generation in the target development system upon role approval.

These approved roles can then be moved from development towards the quality assurance and eventually to the PROD systems using standard SAP transport mechanisms.

With its ability to analyze access risks in all role definitions and automatically provision roles to SAP applications, Virsa Role Expert contributes unique functionality to SAP GRC Access Control.

Virsa Access Enforcer is typically deployed against the production enterprise system to provision new users or change access of existing users in the production environment. The Virsa Access Enforcer RTA ensures automatic provisioning of users into the SAP applications upon approval of the access in Virsa Access Enforcer.

Virsa FireFighter for SAP can grant privileged access to select users, which could not be accomplished from outside the target applications. It is typically deployed on the production system to ensure proper super-user handling. Only the reporting component runs outside of the SAP application.

SAP GRC Access Control users and their authorizations are maintained in the standard SAP user-management engine for all Java applications.

Authoritative-User Sources

For user provisioning, Virsa Access Enforcer supports several alternative options as the authoritative-user source:

- **LDAP directory servers**
  Many customers do not create users using SAP HR functionality but use an LDAP directory server (Microsoft Active Directory or something similar) to maintain the authoritative-user source information for all employees and contractors. In this scenario, Virsa Access Enforcer can pull information from LDAP directories and then run the compliant provisioning, including risk analysis, approval workflows, mitigation, and ultimately automated provisioning of the approved-user access into the target PROD system.
- **mySAP ERP HCM** (either a separate SAP HR application or directly from the PROD system)
  Similarly, if you are using mySAP ERP HCM to maintain user information, Virsa Access Enforcer can pull information from mySAP ERP HCM, run compliant-provisioning steps, and provision that data to the target application. In this case, the mySAP ERP HCM solution not only serves as the authoritative source, but can also trigger provisioning based on HR events.
- **SAP user-management engine**
  Similarly, the SAP user-management engine can be used as a source for user information feeding into the compliant-provisioning process.

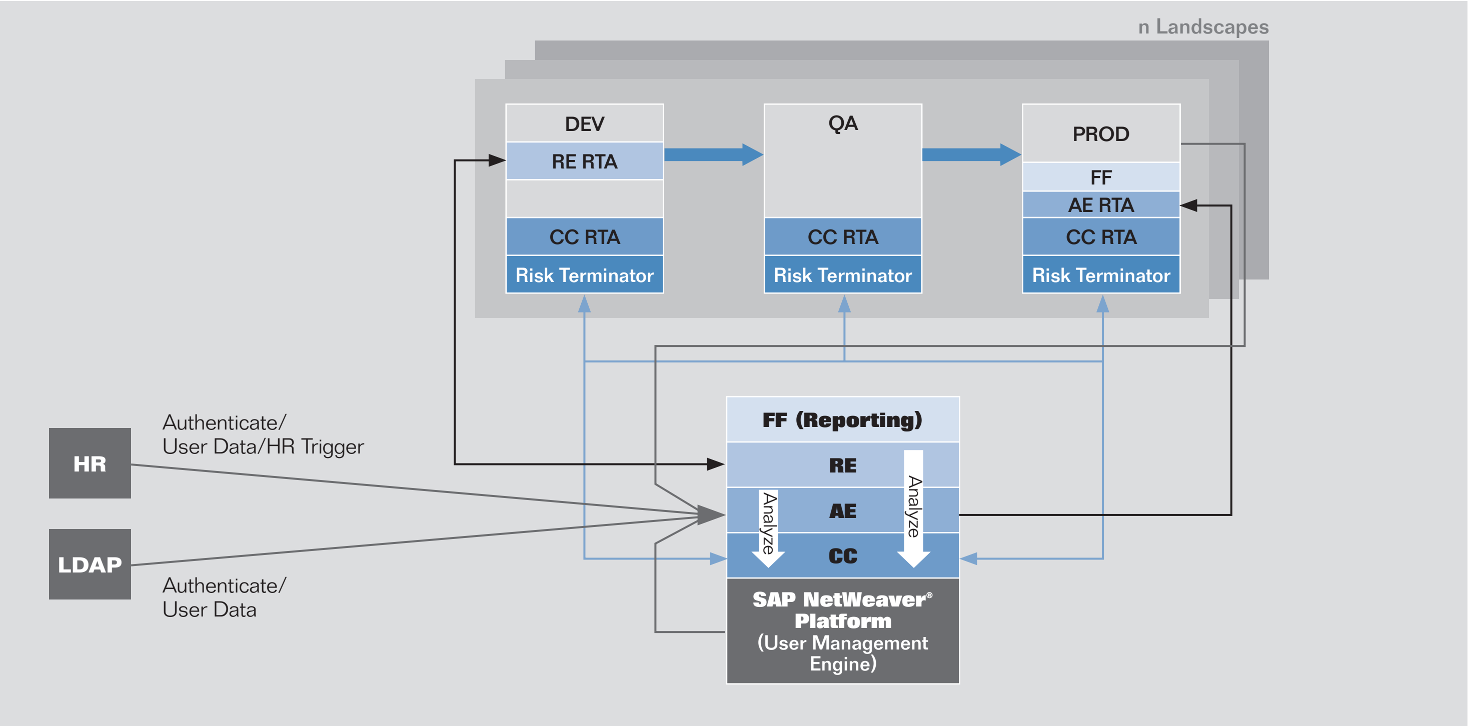


Figure 8: SAP® GRC Access Control Application System Landscape with Authoritative-User Sources

Compliant User Provisioning

Virsa Access Enforcer supports two options for user provisioning:

- Directly to the SAP software PROD system
- Indirectly, via the SAP central user administration (CUA) application

The CUA application is typically used by those enterprises running more than one SAP application landscape. Since Virsa Access Enforcer is a product to provision users, and CUA is a product to provision users, how do these two work together? Virsa Access Enforcer can directly provision into the target systems, eliminating the need for the CUA. In this case, Virsa Access Enforcer provisions one target system at a time. If one user needs to be created or changed in more than one target application, multiple user-provisioning requests are needed.

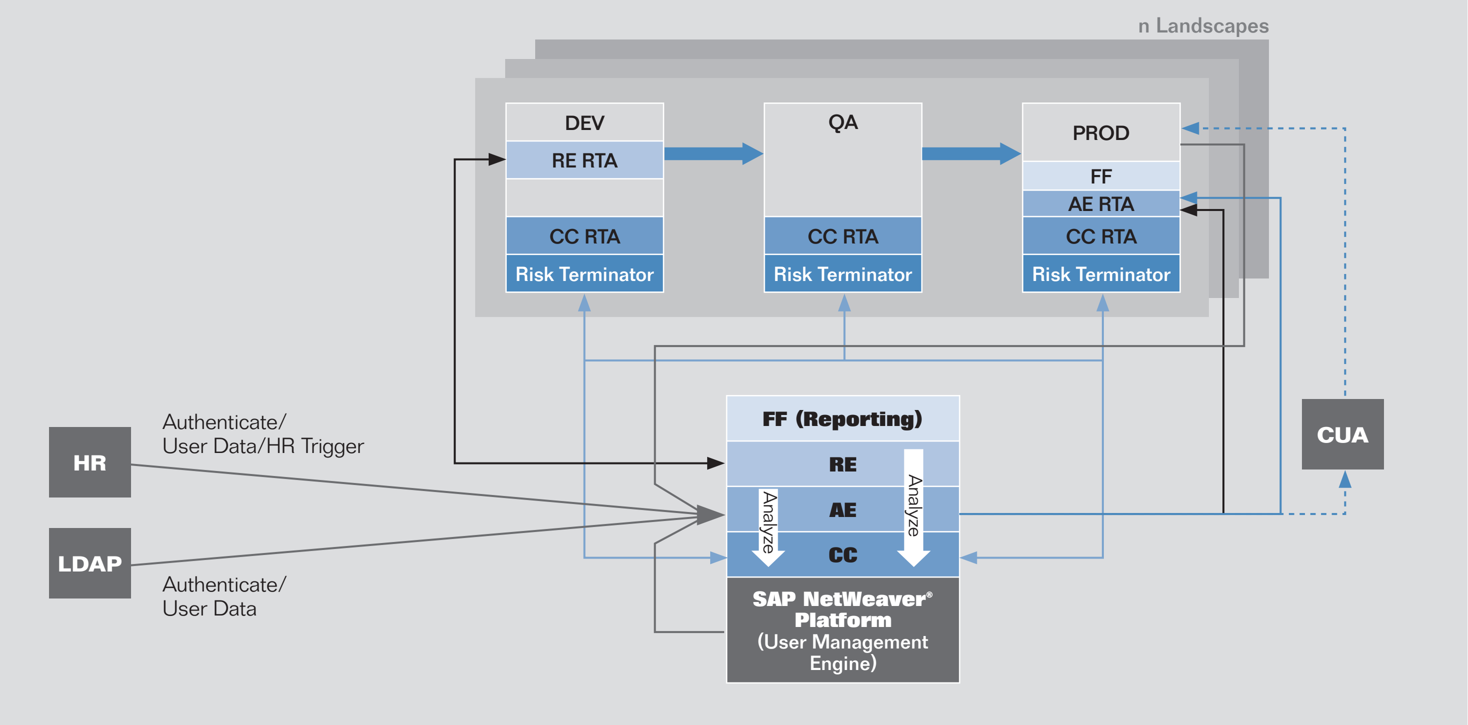


Figure 9: SAP® GRC Access Control Application System Landscape with User Provisioning with or Without the Central User Administration

Alternatively, Virsa Access Enforcer can provision users into the CUA; the CUA in turn provisions to the various target landscapes. In this case, a user that needs to be created or changed in multiple target applications requires only one provisioning request in Virsa Access Enforcer.

Non-SAP Software System Landscapes

Similar deployment scenarios are supported for non-SAP software system landscapes. SAP GRC Access Control is cross-enterprise-ready and the SAP partner ecosystem has already delivered a range of RTAs for enterprise software systems such as Oracle, PeopleSoft, JD Edwards EnterpriseOne, and Hyperion. For detailed information on the out-of-the-box functionality of SAP GRC Access Control and partner RTAs in the various target environments, please refer to the table at the end of this document.

Should your enterprise software system not be among those currently supported out of the box, please contact the SAP GRC services organization for help with custom RTAs and extractors.

HARDWARE AND PERFORMANCE CONSIDERATIONS

In a typical installation, SAP GRC Access Control can be deployed on a single SAP NetWeaver server. However, for enterprises with a larger number of users and processing requirements that put a heavier load on the system, SAP GRC Access Control can be deployed across an SAP NetWeaver cluster. Running in a clustered environment provides essential load balancing and failover capabilities. In addition, clustering will increase the availability of the solution and allow the system to be easily scaled.

Hardware Requirements

The following sections describe typical hardware requirements based on average customer deployments. Actual results may vary.

Virsa Compliance Calibrator

The minimum hardware requirements to support a Virsa Compliance Calibrator deployment are:

- Web application server: SAP J2EE Java Stack 640 (ABAP™ programming language option) and up with Internet Graphics Server
- System type: Server
- Processor: IA 386 or equivalent (dual processor or above)
  Processor speed: 2.40 GHz, 3.06 GHz, 3.20 GHz or above
- RAM:
  For a pure Java instance of the Web application server:
  4 GB or above
  For a combined Java and ABAP Web application server:
  6 GB or above
  Extending an existing ABAP Web application server with
  a Java instance: Add 2 GB
  (This recommendation is a guideline that assumes that the configuration is a central system with a central database and central services instance running on the same host machine.)
- Disk storage:
  Recommended disk space is 120 GB or above, which supports a 3-year operation horizon.
  Minimum disk space is 40 GB to get started.

Other Virsa Compliance Calibrator hardware-sizing considerations include the following:

- One SoD violation consumes about 1.5 MB of disk space. Therefore, 1,000 violations will take about 1.5 GB of space and so on.
- The number of SoD violations depends upon the number of users, roles per user, and the number of SAP and non-SAP software systems for which analysis is being carried out.
- Sizing is also impacted by the following factors. As these factors increase, so will the sizing requirements:
  - Whether the risk analysis is to be run in real time or offline
  - Total number of systems or applications included
  - Number of users
  - Number of roles
  - Number of authorizations
  - Number of tables that must be maintained

Virsa Access Enforcer

The minimum hardware requirements for a Virsa Access Enforcer deployment are:

- Web application server: SAP J2EE Java Stack 640 (ABAP option) and up with Internet Graphics Server
- System type: Server
- Processor: IA 386 or equivalent (dual processor or above)
  Processor speed: 2.40 GHz, 3.06 GHz, 3.20 GHz or above
- RAM:
  For a pure Java instance of the Web application server:
  4 GB or above
  For a combined Java and ABAP Web application server:
  6 GB or above
  Extending an existing ABAP Web application server with
  a Java instance: add 2 GB
- Disk storage:
  Recommended disk space is 120 GB or above, which supports a 3-year operation horizon.
  Minimum disk space is 40 GB to get started.

The sizing requirements for Virsa Access Enforcer are impacted by the anticipated number of:

- User-access change requests
- New user requests

Virsa Role Expert

The minimum hardware requirements to support SAP GRC Access Control role management functionality are:

- Web application server: SAP J2EE Java Stack 640 (ABAP option) and up with Internet Graphics Server
- System type: Server
- Processor: IA 386 or equivalent (dual processor or above)
  Processor speed: 2.40 GHz, 3.06 GHz, 3.20 GHz or above
- RAM:
  For a pure Java instance of the Web application server: 4 GB or above
  For a combined Java and ABAP Web application server: 6 GB or above
  Extending an existing ABAP Web application server with a Java instance: add 2 GB
- Disk storage:
  Recommended disk space is 120 GB or above, which supports a 3-year operation horizon.
  Minimum disk space is 40 GB to get started.

Virsa FireFighter for SAP

Hardware requirements are minimal, as this functionality is deployed on your ABAP stack and reuses SAP software log information.

Combined Deployment

If you combine one or more of these applications on the same hardware, the above requirements for processor and memory are not cumulative. Disk storage space should be added for the respective applications.

Software Requirements

SAP GRC Access Control supports all operating and database software systems supported by SAP NetWeaver. For further details, please refer to the product availability matrix on the SAP Service Marketplace extranet (service.sap.com).

OS	DATABASE
Winx86_64	MSSQL
Win32	MaxDB
Linux PPC	MaxDB
zLinux	DB2
HP-UX	MaxDB
AIX	Oracle
OS400	DB2
WinIA64	Oracle
Linux_x86_64	DB2
HP-UX	DB2

Figure 10: Operating Systems and Databases Supported by the SAP® GRC Access Control Application

MEETING COMPLIANCE REQUIREMENTS WITH SAP GRC ACCESS CONTROL

SAP GRC Access Control delivers a well-rounded access and authorization solution that extends from design time (role design) to runtime (streamlined compliant user provisioning), leaving no gaps for access risk violations in between. Whether used stand-alone or as a core element of SAP solutions for GRC, SAP GRC Access Control ensures compliance with a wide range of internal policies and external regulations to address the basic need of proper access management.

SAP solutions for GRC present an alternative to the fragmented point solutions available in the market. SAP GRC Access Control makes access and authorization risk management and compliant user provisioning an integral part of any company's business and IT strategies. By embedding compliance into business processes, SAP is making compliance repeatable, sustainable, and less costly for companies of all sizes in all industry segments.

This end-to-end solution drives the value of a comprehensive strategy for controlling and addressing future governance, risk, and compliance areas. The benefits of this comprehensive approach include:

- **Intelligent IT risk management:** Delivered through an intelligent network infrastructure that can provide IT risk management information and controls at high speeds throughout the enterprise
- **Improved business performance and predictability:** Achieved through comprehensive visibility, a systematic process for anticipating and controlling risks, and the tools to proactively determine proper actions and critical tasks
- **Optimized risk–return portfolios:** Achieved with transparency and insight for selecting (and rejecting) projects based on risk impact and probability relative to potential return
- **Reduced GRC costs:** Accomplished by significantly cutting down the resources required to control and address risk, ensure compliance, and maintain effective governance
- **Business sustainability:** Delivered through software automation, analytics, and alerts; visibility to risk interdependencies for improved control; and repeatable, cost-effective GRC solutions
- **Business agility:** Achieved by empowering decision makers to identify and assess alternative what-if and future scenarios, leading to greater business agility and competitiveness
- **Increased shareholder value:** Delivered through good governance – reflected in many intangibles, including brand, culture, and reputation – that can have a favorable impact on share-price premiums

SAP GRC Access Control is a proven solution with over 500 customers, making it the number-one solution in the market based on customer adoption. SAP offers a full range of associated GRC services for companies that need to integrate legacy solutions or custom applications. Through these services, you can extend the benefits of the SAP solutions for GRC to your entire enterprise.

SAP offers a variety of "quick start" programs that will get your SAP GRC Access Control solution up and running and bring your enterprise into critical compliance in less than two weeks.

SAP has long recognized the growing role of enterprise systems in assisting companies to meet the increasing challenges of corporate compliance and risk management. Customers are looking for powerful compliance solutions that work across heterogeneous IT environments to reduce risk and cost as well as provide improved business control. SAP provides the most comprehensive set of applications for managing and preventing user-access and authorization risk, enabling customers to comply with regulatory requirements and maintain high standards of governance and risk management, while minimizing cost and complexity. To learn more about how SAP can help your GRC initiatives, call your SAP representative today or visit us on the Web at www.sap.com/grc.

APPENDIX: PROCESSES AND APPLICATIONS SUPPORTED

SAP® GRC Access Control Product Functionality Across Target Enterprise Software Systems

SAP GRC ACCESS CONTROL				
SAP	**Oracle**	**PeopleSoft**	**JD Edwards**	**Hyperion**
■ HR ■ Procure to Pay ■ Order to Cash ■ Finance – General Accounting – Project Systems – Fixed Assets ■ Basis, Security, and System Administration ■ Materials Management ■ Advanced Planning and Optimization ■ Supplier Relationship Management ■ Customer Relationship Management ■ Consolidations	■ HR ■ Procure to Pay ■ Order to Cash ■ Finance – General Accounting – Project Systems – Fixed Assets ■ System Administration	■ HR ■ Procure to Pay ■ Order to Cash ■ Finance – General Accounting – Fixed Assets ■ System Administration	■ HR/Payroll ■ Procure to Pay ■ Order to Cash ■ Finance – General Accounting ■ Consolidations	■ Custom Rules

www.sap.com/contactsap

THE BEST-RUN BUSINESSES RUN SAP™